Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019287

International filing date: 16 December 2004 (16.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-003431
Filing date: 08 January 2004 (08.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2004/019287

16.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

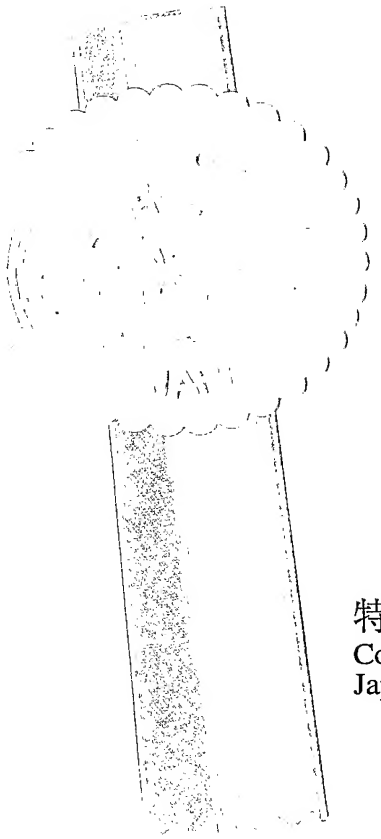
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月　８日

出願番号
Application Number: 特願２００４－００３４３１

[ST. 10/C]: [ＪＰ２００４－００３４３１]

出願人
Applicant(s): 松下電器産業株式会社



２００５年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００４０２４

【書類名】　特許願
【整理番号】　2048160002
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00　640
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　庭野　智
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　岡本　隆一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　徳田　克己
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　村上　弘規
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、
前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する少なくとも１つのフォーマット変換手段を有すること特徴とするコンテンツ配信システム。
【請求項２】
前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項３】
前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項４】
前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換すること特徴とする請求項３に記載のコンテンツ配信システム。
【請求項５】
前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項６】
前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項７】
前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有すること特徴とする請求項６に記載のコンテンツ配信システム。
【請求項８】
前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスＩＤを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスＩＤを復元し、前記ライセンスＩＤでライセンスを管理することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項９】
暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信

するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、

前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換するフォーマット変換すること特徴とするライセンス配信方法。

【請求項１０】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信し、前記ライセンス中継サーバが、前記伝送用のフォーマットのライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記変換フォーマット指定情報に基づき前記伝送用のフォーマットのライセンスを前記処理に用いるフォーマットのライセンスに変換することを特徴とする請求項９に記載のライセンス配信方法。

【請求項１１】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信し、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットにおけるデジタル署名を用いて、前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを署名検証すること特徴とする請求項９に記載のライセンス配信方法。

【請求項１２】

前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスＩＤを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスＩＤを復元し、前記ライセンスＩＤでライセンスを管理することを特徴とする請求項９に記載のライセンス配信方法。

【請求項１３】

暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、

前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する少なくとも１つのフォーマット変換手段を有すること特徴とする端末装置。

【請求項１４】

前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換すること特徴とする請求項１３に記載の端末装置。

【請求項１５】
前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有すること特徴とする請求項１３に記載の端末装置。

【書類名】明細書
【発明の名称】コンテンツ配信システム、ライセンス配信方法および端末装置
【技術分野】
【０００１】
本発明は、放送および通信を用いて、暗号化した映像、音楽などのデジタルコンテンツ（以下コンテンツと記述）と、少なくともコンテンツの利用条件とコンテンツの暗号化に用いたコンテンツ鍵を含むライセンスを配信し、ユーザが端末装置でコンテンツを利用するシステムに関し、特に、受信したライセンスのフォーマットを変換する端末装置を含むシステムに関する。
【背景技術】
【０００２】
近年、デジタルネットワークにより、ユーザの端末装置にコンテンツを配信するシステムが提案されている。ここで、端末装置とは、少なくともＣＰＵと、メモリと、端末装置を制御するソフトウェアから構成される機器のことである。このようなコンテンツ配信システムでは、コンテンツはコンテンツ提供者からユーザの端末装置へ暗号化して配信され、コンテンツを購入したユーザの端末装置にはライセンスが配信される。ここで、ライセンスとは、少なくともコンテンツの利用条件とコンテンツの暗号化に用いたコンテンツ鍵を含むデータであり、例えば、コンテンツ提供者などがライセンス発行者として生成する。
【０００３】
コンテンツの利用条件には、例えば、“３回利用可能“などの、コンテンツの利用に関する条件が記述されている。端末装置には、ライセンスの利用条件からコンテンツの利用可否を判定し、コンテンツ鍵の利用を制御する、ライセンス処理部がある。
このように、ライセンスにより、ライセンス発行者の意図したとおりのコンテンツ利用を実現する方法はＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）と呼ばれ、複数のＤＲＭ方式が提案されている。
【０００４】
コンテンツを提供するコンテンツ提供者には、ユーザによるコンテンツ購入機会拡大のため、複数の配信経路で暗号化コンテンツおよびライセンスを配信したいという要求があり、放送および通信で配信する方法が提案されている。
通常、ライセンスのフォーマットと、ライセンスの処理方法は、ＤＲＭ方式の方式設計者により規定されるが、例えば、放送では総務省によりコンテンツ鍵の伝送方法が一部規定されているように、ＤＲＭ方式の方式設計者以外の、例えば、配信事業者などによりライセンスの伝送路上でのフォーマット（以下伝送フォーマットと記述）が一部規定されることがあり、１つのＤＲＭ方式でも、配信経路に応じてライセンスの伝送フォーマットを変更する場合がある。
【０００５】
従来、特許文献１などに開示されているように、端末装置内での利用条件の処理を共通化するために、配信業者毎に利用条件のフォーマットが異なる場合には、受信した利用条件を内容が同一の統一フォーマットに変換している。
【特許文献１】特開２００１－２０２０８８号公報
【非特許文献１】ウォーウィック・フォード＋マイケル・バウム著「デジタル署名と暗号技術」　株式会社ピアソン・エデュケーション　１９９７年
【発明の開示】
【発明が解決しようとする課題】
【０００６】
端末装置が複数の伝送フォーマットのライセンスを受信する場合には、受信した伝送フォーマットのライセンスを共通の処理用のフォーマット（以下処理フォーマットと記述）に変換することで、ライセンス処理を共通化できるため、端末装置内の処理を効率化することができる。

しかし、端末装置で複数のＤＲＭ方式でライセンスを処理する場合には、ＤＲＭ方式毎にセキュリティを確保することが必要なため、それぞれのＤＲＭ方式のライセンス処理部で独自にライセンスを処理することから、ＤＲＭ方式毎に処理フォーマットが異なることがある。また、ＤＲＭ方式によっては、サービス毎に処理を分けるなどの理由から、１つのＤＲＭ方式でも複数の処理フォーマットを規定することもある。

【０００７】

従来の方法では、端末装置がライセンスを処理フォーマットに変換する場合に、ライセンス発行者がライセンス毎にライセンス処理フォーマットを指定することができないという課題を有していた。

さらに、ライセンス発行者がライセンス毎に端末装置でのライセンス処理フォーマットを指定することができたとしても、端末装置におけるフォーマット変換で生成されたライセンスの改ざん検出ができないという課題がある。

【０００８】

そして、同じライセンス処理部に対して配信経路に応じて異なるフォーマットで配信したライセンスも配信後は統一的に管理したいという課題がある。

本発明は、こうした従来の問題点を解決するものであり、端末装置でライセンスのフォーマット変換を行うコンテンツ配信システムにおいて、ライセンス発行者によるライセンスの変換フォーマットの指定と、フォーマット変換で生成されたライセンスの改ざん検出と、異なるフォーマットで配信されたライセンスの配信後の統一的な管理を可能とするコンテンツ配信システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

本発明の請求項１記載のコンテンツ配信システムは、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換するフォーマット変換手段を有する。

【００１０】

本発明の請求項２記載のコンテンツ配信システムは、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信する。

本発明の請求項３記載のコンテンツ配信システムは、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納する。

【００１１】

本発明の請求項４記載のコンテンツ配信システムは、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換する。

本発明の請求項５記載のコンテンツ配信システムは、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信する。

【００１２】

本発明の請求項６記載のコンテンツ配信システムは、前記ライセンス中継サーバが、前

記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納する。

本発明の請求項７記載のコンテンツ配信システムは、前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有する。

【００１３】

本発明の請求項８記載のコンテンツ配信システムは、前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスＩＤを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスＩＤを復元し、前記ライセンスＩＤでライセンスを管理する。

【００１４】

本発明の請求項９記載のライセンス配信方法は、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する。

【００１５】

本発明の請求項１０記載のライセンス配信方法は、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信し、前記ライセンス中継サーバが、前記伝送用のフォーマットのライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記変換フォーマット指定情報に基づき前記伝送用のフォーマットのライセンスを前記処理に用いるフォーマットのライセンスに変換する。

【００１６】

本発明の請求項１１記載のライセンス配信方法は、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信し、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットにおけるデジタル署名を用いて、前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを署名検証する。

【００１７】

本発明の請求項１２記載のライセンス配信方法は、前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスＩＤを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスＩＤを復元し、前記ライセンスＩＤでライセンスを管理する。

【００１８】

本発明の請求項１３記載の端末装置は、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも１種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管

理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する。

【００１９】

本発明の請求項１４記載の端末装置は、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換する。

【００２０】

本発明の請求項１５記載の端末装置は、前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有する。

【発明の効果】

【００２１】

本発明の変換フォーマット指定情報によれば、端末装置での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスも、端末装置のフォーマット変換手段が、ライセンスに含まれる変換フォーマット指定情報により指定されるフォーマットのライセンスに変換するため、ライセンス発行者による端末装置におけるライセンスの処理フォーマットの指定と、端末装置における受信後のライセンス処理の共通化が可能になる。

【００２２】

また、本発明の処理に用いるフォーマットにおけるデジタル署名により、端末装置での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスを処理に用いるフォーマットに変換した後にデジタル署名によるライセンスの改ざん検出が可能となる。

さらに、ライセンス発行者が生成したライセンスＩＤと一致するライセンスＩＤをフォーマット変換後のライセンスで復元することにより、異なるフォーマットで配信されたライセンスをライセンス発行者が統一的に管理することが可能となる。

【発明を実施するための最良の形態】

【００２３】

以下、本発明の実施の形態について、図面を参照しながら説明する。

尚、以下の説明に記述されるコンテンツの暗号化方式は、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＴｒｉｐｌｅ ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等の共通鍵暗号アルゴリズムが、デジタル署名の方式には、ＲＳＡやＥＣ－ＤＳＡ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）等の公開鍵暗号アルゴリズムが用いられるのが一般的であり、以下に説明する処理は特定の暗号方式に依存しない。また、ハッシュ計算方式は、ＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）やＭＤ５等が用いられるのが一般的であり、本実施の形態は特定のハッシュ計算方式に依存しない。

【００２４】

また、本実施の形態では、ライセンスを送受信する場合には、セキュリティを確保するため、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）などの安全な認証チャネル（Ｓｅｃｕｒｅ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｃｈａｎｎｅｌ、以下、ＳＡＣと記述）を確立することなどにより、受信側と共有した暗号鍵、または、あらかじめ構成要素間で共有しておいた暗号鍵を用いて少なくともコンテンツ鍵を暗号して通信を行っている。尚、デジタル署名とそれを使った改ざん検出、および、ＳＡＣについては、非特許文献１など

が詳しい。

【００２５】

図１は、本発明の実施の形態に関わるコンテンツ配信システム１の全体の構成を示す図である。図１に示すように、コンテンツ配信システム１は、ライセンス管理サーバ１００と、ライセンス中継サーバ１１０と、端末装置１２０と、コンテンツ配信サーバ１３０とを備え、各々が伝送路Ｎで接続されている。

ライセンス管理サーバ１００は、コンテンツ提供者等のライセンス発行者側に設置される装置であって、少なくとも、コンテンツ配信サーバ１３０からのコンテンツ情報の受信と、ライセンスの作成と、ライセンス中継サーバ１１０へのライセンスの送信と、端末装置１２０へのライセンスの配信とを行う。コンテンツ情報とは、少なくとも、コンテンツＩＤと、コンテンツ鍵を含むデータである。

【００２６】

ライセンス中継サーバ１１０は、配信事業者等に設置される装置であって、少なくとも、ライセンス管理サーバ１００からのライセンス生成情報の受信と、ライセンス生成情報からライセンスへの変換と、端末装置１２０へのライセンスの配信を行う。

端末装置１２０は、少なくとも、暗号化コンテンツとライセンスの受信と、ライセンスの伝送フォーマットから処理フォーマットへの変換と、暗号化コンテンツの利用を行う。

【００２７】

コンテンツ配信サーバ１３０は、コンテンツ提供者等に設置される装置であって、少なくとも、暗号化コンテンツの生成と、コンテンツ情報のライセンス管理サーバ１００への送信と、暗号化コンテンツの端末装置１２０への送信を行う。

伝送路Ｎは、インターネット等の通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

【００２８】

尚、コンテンツ配信システム１には、公開鍵証明書、および、共有する暗号鍵などの管理を行う図示しないＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）サーバ、および、鍵管理サーバなども接続されているが、本実施の形態では、詳しく説明しない。

次に、コンテンツ配信システム１の各構成要素について説明する。

（構成要素１）ライセンス管理サーバ１００

図２は、本発明の実施の形態におけるライセンス管理サーバ１００の構成を示す図である。

【００２９】

図２において、コンテンツ情報受信部２１０は、コンテンツ配信サーバ１３０から、コンテンツ情報を受信する。

ライセンス生成部２２０は、少なくともコンテンツ情報と、ライセンス発行者が設定した利用条件から、端末装置１２０に配信する処理フォーマットライセンス５１０と、ライセンス中継サーバ１１０に送信するライセンス生成情報を生成する。

【００３０】

ライセンス送信部２３０は、ライセンス中継サーバ１１０にライセンス生成情報を、端末装置１２０に処理フォーマットライセンス５１０をそれぞれ送信する。

（構成要素２）ライセンス中継サーバ１１０

図３は、本発明の実施の形態におけるライセンス中継サーバ１１０の構成を示す図である。

【００３１】

図３において、ライセンス生成情報受信部３１０は、ライセンス管理サーバ１００からライセンス生成情報を受信する。

ライセンス変換部３２０は、ライセンス管理サーバ１００から受信したライセンス生成情報を変換し、伝送フォーマットライセンス７１０を生成する。

ライセンス送信部３３０は、伝送フォーマットライセンス７１０を端末装置１２０に送信する。

【００３２】
尚、本実施の形態では、ライセンス中継サーバ１１０が伝送フォーマットライセンス７１０を生成する場合について記述するが、ライセンス管理サーバ１００のライセンス生成部２２０で伝送フォーマットライセンス７１０を生成する場合には、ライセンス変換部３２０がライセンス管理サーバ１００に含まれ、ライセンス生成情報受信部３１０で伝送フォーマットライセンス７１０を受信することになるが、同様な効果が得られる。
【００３３】
（構成要素３）端末装置１２０
端末装置１２０は、耐タンパ部４１０と、図示しないノンセキュア部から構成される。

ノンセキュア部は少なくともユーザインタフェースなどの処理を行う。以上で端末装置１２０のノンセキュア部について説明した。
【００３４】
図４は、本発明の実施の形態における端末装置１２０の耐タンパ部４１０の構成を示す図である。
図４において、耐タンパ部４１０は、第１のライセンス処理部４２０と、第２のライセンス処理部４２１と、コンテンツ処理部４５０から構成されている。
第１のライセンス処理部４２０は、伝送フォーマットライセンス７１０の受信と、ライセンスのフォーマット変換を行う伝送フォーマットＡライセンス変換部４３０と、伝送フォーマットＢライセンス変換部４３１と、処理フォーマットライセンス５１０の受信と、ライセンス判定処理を行う処理フォーマットαライセンス判定部４４０と処理フォーマットβライセンス判定部４４１から構成されている。
【００３５】
ここで、ライセンス判定処理とは、利用条件判定と、少なくともコンテンツ鍵のコンテンツ処理部４５０への送信を意味する。
尚、耐タンパ部４１０の端末装置１２０への実装は、端末装置１２０から取り外せない状態で実装する場合と、ＩＣカードなどの可搬型モジュールとして実装する場合があるが、本発明は、どちらの実装でも同様な効果が得られる。
【００３６】
尚、本実施の形態では、１つの耐タンパ部４１０に第１のライセンス処理部４２０と、コンテンツ処理部４５０が実装されているが、第１のライセンス処理部４２０と、コンテンツ処理部４５０の間で送受信されるデータがＳＡＣなどにより安全に保護されるならば、異なる耐タンパ部に実装されても同様な効果が得られる。
尚、本実施の形態では、第１のライセンス処理部４２０が伝送フォーマットＡと、伝送フォーマットＢと、処理フォーマットαと、処理フォーマットβに対応する場合について記述するため、第１のライセンス処理部４２０が、伝送フォーマットＡライセンス変換部４３０と、伝送フォーマットＢライセンス変換部４３１と、処理フォーマットαライセンス判定部４４０と処理フォーマットβライセンス判定部４４１とから構成されているが、ライセンス処理部には、少なくとも１つの伝送フォーマットライセンス変換部と、１つの処理フォーマットライセンス判定部があれば同様な効果が得られる。
【００３７】
第２のライセンス処理部４２１は、第１のライセンス処理部４２０とは異なるＤＲＭ方式のライセンスを処理するが第１のライセンス処理部４２０と同様な構成であり、本実施の形態では詳しく説明しない。
尚、本実施の形態では、２つのＤＲＭ方式に対応した端末装置１２０について記述するため、耐タンパ部４１０に第１のライセンス処理部４２０と第２のライセンス処理部４２１があるが、少なくとも１つのライセンス処理部があれば同様な効果が得られる。
【００３８】
コンテンツ処理部４５０は、暗号化コンテンツをコンテンツ鍵で復号し、利用条件に基づき利用処理を行う。

尚、本実施の形態では、端末装置１２０にコンテンツ処理部４５０が１つの場合について記述するが、ＤＲＭ方式毎に異なるコンテンツ処理部４５０がある場合も同様な効果が得られる。

【００３９】

（構成要素４）コンテンツ配信サーバ１３０

コンテンツ配信サーバ１３０は、コンテンツ情報と暗号化コンテンツ８１０を生成し、コンテンツ情報をライセンス管理サーバ１００に、暗号化コンテンツ８１０を端末装置１２０に配信する。

次に、コンテンツ配信システム１の各構成要素が保有するデータについて説明する。

【００４０】

（データ１）処理フォーマットライセンス５１０

図５は処理フォーマットライセンス５１０の記述例である。

処理フォーマットライセンス５１０は、少なくとも端末装置１２０の耐タンパ部４１０での処理に用いられる。また、処理フォーマットライセンス５１０は、ライセンス本体５１１と、処理フォーマット署名５１２とから構成されている。

【００４１】

ライセンス本体５１１には利用条件、および、コンテンツ鍵が記述される。

処理フォーマット署名５１２には、ライセンス本体５１１に対するライセンス発行者のデジタル署名が記述され、ライセンス本体５１１の改ざん検出に用いる。

図６はＸＭＬ言語によるライセンス本体５１１と処理フォーマット署名５１２の記述例である。

【００４２】

尚、本実施の形態では、処理フォーマットライセンス５１０の記述例としてＸＭＬ言語で記述された例を示すが、少なくとも、利用条件とコンテンツ鍵が記述できれば他の記述形式でもよい。

図６において、＜ｒｉｇｈｔ＞はコンテンツの再生または他のメディアへの移動などの利用方法を、＜ｃｏｎｔｅｎｔＩＤ＞はコンテンツの識別に用いるコンテンツＩＤを、＜ｃｏｎｔｅｎｔＫｅｙ＞は暗号化コンテンツの復号に用いるコンテンツ鍵を、＜ｍａｘＣｏｕｎｔ＞はコンテンツの最大利用回数を、＜ｄｒｍＩＤ＞はＤＲＭ方式を特定する識別子を、＜ｖｅｒｓｉｏｎ＞はライセンスフォーマットのバージョンを、＜ｌｉｃｅｎｓｅＩＤ＞はライセンスの識別に用いるライセンスＩＤを、＜ｅｎｄＴｉｍｅＰｏｉｎｔ＞はライセンスの終了時間を、＜ｓｉｇｎａｔｕｒｅ＞は処理フォーマット署名５１２を示し、このライセンスが、“０００１”というＤＲＭ方式の、Ｖｅｒ１．０のライセンスフォーマットで記述された、“０２”というＩＤのライセンスであり、　“０２”　というＩＤのコンテンツを、２００３年８月３１日１２時３４分５６秒まで、最大９回利用可能で、このコンテンツ復号に必要なコンテンツ鍵が０００１であることを示している。

【００４３】

尚、タグを追加することで、図６に示す以外の情報項目を追加することができる。

（データ２）伝送フォーマットライセンス７１０

図７は、ライセンス中継サーバ１１０が、ライセンス管理サーバ１００から受信したライセンス生成情報を基に生成する、図６の処理フォーマットライセンスの記述例と同一内容の、伝送フォーマットライセンス７１０の記述例である。

【００４４】

伝送フォーマットライセンス７１０は、変換フォーマット指定情報７１１と、処理フォーマット署名７１２と、ライセンス本体７５０と、改ざん検出７６０から構成される。

変換フォーマット指定情報７１１は、端末装置１２０の伝送フォーマットライセンス変換部で、伝送フォーマットライセンス７１０の処理フォーマット署名７１２と、ライセンス本体７５０に含まれる情報項目を処理フォーマットに変換する際の変換フォーマットを指定する情報であり、例えば、処理フォーマットαに変換する場合には、処理フォーマットαを特定する識別子“α”が格納される。

【００４５】
尚、本実施の形態では、変換フォーマット指定情報７１１が処理フォーマットを特定する識別子の場合について記述するが、処理フォーマットが１つしかないＤＲＭ方式では、変換するか否かの２値を指定するフラグでも同様な効果が得られる。
処理フォーマット署名７１２は、処理フォーマットライセンス５１０の処理フォーマット署名５１２と同じデータである。
【００４６】
ライセンス本体７５０は、ライセンス本体５１１に相当する内容であり、本実施の形態では、ｄｒｍＩＤ７１６が＜ｄｒｍＩＤ＞に、ｖｅｒｓｉｏｎ７１９が＜ｖｅｒｓｉｏｎ＞に、ｌｉｃｅｎｓｅＩＤ７２２が＜ｌｉｃｅｎｓｅＩＤ＞に、ｒｉｇｈｔ７２５が＜ｒｉｇｈｔ＞に、ｍａｘＣｏｕｎｔ７２８が＜ｍａｘＣｏｕｎｔ＞に、ｃｏｎｔｅｎｔＩＤ７３１が＜ｃｏｎｔｅｎｔＩＤ＞に、ｃｏｎｔｅｎｔＫｅｙ７３４が＜ｃｏｎｔｅｎｔＫｅｙ＞に、ｅｎｄＴｉｍｅＰｏｉｎｔ７３７が＜ｅｎｄＴｉｍｅＰｏｉｎｔ＞に、それぞれ対応する値が格納される。
【００４７】
尚、端末装置１２０でのフォーマット変換後のライセンス本体５１１が、ライセンス管理サーバ１００で生成したライセンス本体５１１と一致するならば、ライセンス本体７５０の各値は、ライセンス本体５１１の対応する値と異なる場合でも同様な効果が得られる。したがって、フォーマット変換の変換規則をライセンス中継サーバ１１０と端末装置１２０が共有していれば、例えば、ライセンス本体５１１のライセンスＩＤが“０２”であり、本実施の形態では説明しないライセンス中継サーバ１１０の識別番号が“０１”であり、ライセンス本体７５０のライセンスＩＤが、ライセンス本体５１１におけるライセンスＩＤの先頭にライセンス中継サーバ１１０の識別番号が付加するという変換規則により、“０１０２”となる場合でも、端末装置１２０でライセンス本体７５０からライセンス本体５１１にフォーマット変換する時に、ライセンス中継サーバ１１０の識別番号に対応するライセンス本体７５０のライセンスＩＤの先頭部分“０１”を削除することで、ライセンス本体５１１のライセンスＩＤを“０２”にすることができれば、同様な効果が得られる。
【００４８】
尚、本実施の形態では、ライセンス本体５１１と、ライセンス本体７５０の対応する値は一致しているが、以下の説明ではライセンス本体の各値については説明しない。
記述子タグ７１４には、ｄｒｍＩＤを特定する識別子が、記述子長７１５には、ｄｒｍＩＤ７１６のバイト長が、記述子タグ７１７には、ｖｅｒｓｉｏｎを特定する識別子が、記述子長７１８には、ｖｅｒｓｉｏｎ７１８のバイト長が、記述子タグ７２０には、ライセンスＩＤを特定する識別子が、記述子長７２１には、ｌｉｃｅｎｓｅＩＤ７２１のバイト長が、記述子タグ７２３には、ｒｉｇｈｔを特定する識別子が、記述子長７２４には、ｒｉｇｈｔ７２５のバイト長が、記述子タグ７２６には、ｍａｘＣｏｕｎｔを特定する識別子が、記述子長７２７には、ｍａｘＣｏｕｎｔ７２８のバイト長が、記述子タグ７２９には、ｃｏｎｔｅｎｔＩＤを特定する識別子が、記述子長７３０には、ｃｏｎｔｅｎｔＩＤ７３１のバイト長が、記述子タグ７３２には、ｃｏｎｔｅｎｔＫｅｙを特定する識別子が、記述子長７３３には、ｃｏｎｔｅｎｔＫｅｙ７３４のバイト長が、記述子タグ７３５には、ｅｎｄＴｉｍｅＰｏｉｎｔを特定する識別子が、記述子長７３６には、ｅｎｄＴｉｍｅＰｏｉｎｔ７３７のバイト長が、それぞれ格納される。
【００４９】
改ざん検出７６０は変換フォーマット指定情報７１１から改ざん検出７６０直前までのバイト列のハッシュ値であり、伝送フォーマットライセンス７１０の改ざん検出に用いる。
尚、本実施の形態では、改ざん検出７１０としてハッシュ値を用いるが、デジタル署名など改ざんの検出が可能なデータであれば、同様な効果が得られる。
【００５０】

尚、伝送フォーマットライセンス７１０には、記述子タグを追加することで、図７に示す以外の情報項目を追加することができる。

尚、本実施の形態では、伝送フォーマットライセンス７１０が記述子形式で記述される場合について説明するが、少なくとも変換フォーマット指定情報７１１と処理フォーマット署名７１２が含まれていれば、他の記述形式でも同様な効果が得られる。

【００５１】

尚、本実施の形態では、伝送フォーマットＡライセンスの例として、伝送フォーマットライセンス７１０を用いるが、他の伝送フォーマットのライセンスも、少なくとも変換フォーマット指定情報７１１と処理フォーマット署名７１２を含む伝送フォーマットライセンス７１０と類似したデータ構造であれば同様な効果が得られる。

（データ３）暗号化コンテンツ８１０

暗号化コンテンツ８１０は、図８に示す通り、コンテンツＩＤ８１１と、コンテンツ本体８１２から構成され、コンテンツ本体８１２はコンテンツ鍵で暗号化されている。

【００５２】

コンテンツＩＤ８１１は、ライセンスと暗号化コンテンツ８１０を対応付けるために用いる。コンテンツ本体８１２は、映像または音楽などのデジタルデータである。

尚、本実施の形態では、暗号化コンテンツ８１０にコンテンツＩＤ８１１を含む場合について説明するが、他の方法により暗号化コンテンツ８１０と処理フォーマットライセンス５１０が対応付けることができれば、暗号化コンテンツ８１０にコンテンツＩＤ８１１を含まない構造でも同様な効果が得られる。

【００５３】

（データ４）ライセンス生成情報

ライセンス生成情報は、伝送フォーマットライセンス７１０を生成するために、ライセンス管理サーバ１００からライセンス中継サーバ１１０に送信されるデータで、少なくとも、変換フォーマット指定情報７１１と、処理フォーマット署名５１２と、図示しないライセンス本体５１１と内容同一のデータから構成される。

【００５４】

尚、ライセンス生成情報のフォーマットは、ライセンス管理サーバ１００とライセンス中継サーバ１１０との間で規定されていれば、どのようなフォーマットを用いても同様な効果が得られる。

次にコンテンツ配信システム１の構成要素の処理について説明する。

コンテンツ配信システム１におけるライセンスの作成までの処理概略は、例えば、図９に示す手順で行われる。

【００５５】

コンテンツ配信サーバ１３０は、コンテンツと、コンテンツ鍵と、コンテンツＩＤ８１１を生成し、コンテンツをコンテンツ鍵で暗号化してコンテンツ本体８１２を生成し、コンテンツＩＤ８１１とコンテンツ本体８１２から暗号化コンテンツ８１０を生成し、少なくともコンテンツＩＤ８１１とコンテンツ鍵を含むコンテンツ情報をライセンス管理サーバ１００に送信（ステップＳ１００）する。

【００５６】

尚、本実施の形態では、コンテンツ配信サーバ１３０からライセンス管理サーバ１００にコンテンツ情報としてコンテンツＩＤ８１１を送信する場合について記述するが、ライセンス管理サーバ１００がコンテンツＩＤ８１１を生成して、コンテンツ配信サーバ１３０に送信し、コンテンツ配信サーバ１３０が暗号化コンテンツとコンテンツＩＤ８１１を関連付けるようにしても同様な効果が得られる。

【００５７】

ライセンス管理サーバ１００は、コンテンツ情報を受信（ステップＳ１１０）し、処理フォーマットライセンス５１０と、ライセンス中継サーバ１１０に送信するライセンス生成情報を生成（ステップＳ１２０）し、ライセンス生成情報をライセンス中継サーバ１１０に送信（ステップＳ１３０）する。

ライセンス中継サーバ１１０は、ライセンス生成情報を受信（ステップＳ１４０）し、伝送フォーマットライセンス７１０を生成（ステップＳ１５０）する。

【００５８】

コンテンツ配信システム１における暗号化コンテンツとライセンスの配信からコンテンツ利用までの処理概略は、例えば、図１０に示す手順で行われる。

コンテンツ配信サーバ１３０は、端末装置１２０に暗号化コンテンツを配信（ステップＳ１６０）する。

端末装置６００は、コンテンツ配信サーバ１３０から暗号化コンテンツを受信（ステップＳ１９０）する。

【００５９】

ライセンス管理サーバ１００は、端末装置１２０に処理フォーマットライセンス５１０を配信（ステップＳ１７０）する。

端末装置６００は、ライセンス管理サーバ１００から処理フォーマットライセンス５１０を受信（ステップＳ２００）し、ライセンスの利用条件などから利用可否を判定（ステップＳ２１０）し、端末装置６００から受信したコンテンツの利用を制御（ステップＳ２２０）する。

【００６０】

ライセンス中継サーバ１１０は、端末装置１２０に伝送フォーマットライセンス７１０を配信（ステップＳ１８０）する。

端末装置６００は、ライセンス中継サーバ１１０から伝送フォーマットライセンス７１０を受信（ステップＳ２３０）し、処理フォーマットライセンスに変換（ステップＳ２４０）し、ライセンスの利用条件などから利用可否を判定（ステップＳ２５０）し、端末装置６００から受信したコンテンツの利用を制御（ステップＳ２６０）する。

【００６１】

次に、各構成要素の処理について図面を用いて説明する。

図１１を用いて、ライセンス管理サーバ１００の処理について説明する。

（コンテンツ情報受信Ｓ１１０）

ライセンス管理サーバ１００は、コンテンツ配信サーバ１３０からコンテンツ情報を受信（ステップＳ１１０）する。

【００６２】

（ライセンス生成Ｓ１２０）

ライセンス発行者は、ライセンス管理サーバ１００に、コンテンツ配信サーバ１３０から受信したコンテンツ情報に対応する利用条件を入力（ステップＳ１２１）する。

ライセンス管理サーバ１００は、コンテンツ配信サーバ１３０から受信したコンテンツ情報と、ライセンス発行者が入力した利用条件から、処理フォーマットでライセンス本体５１１を生成（ステップＳ１２２）し、ライセンス本体５１１に対する処理フォーマット署名５１２を生成（ステップＳ１２３）する。複数の処理フォーマットを持つＤＲＭ方式のライセンス管理サーバ１００では、各処理フォーマットに対してステップＳ１２２からステップＳ１２３の処理フォーマットライセンス５１０の生成を繰り返す（ステップＳ１２４）。

【００６３】

尚、本実施の形態では、第１のライセンス処理部４２０で処理される処理フォーマットαと処理フォーマットβを有するＤＲＭ方式について記述するため、ステップＳ１２４で２つの処理フォーマットライセンス５１０を生成するが、少なくとも１つの処理フォーマットライセンス５１０を生成すれば、同様な効果が得られる。

【００６４】

次に、ライセンス管理サーバ１００は、ライセンス本体５１１を送信先のライセンス中継サーバ１１０とライセンス管理サーバ１００との間で規定されているフォーマットに変換し、各処理フォーマットに対応する処理フォーマット署名５１２と、変換フォーマット指定情報７１１を付加して、ライセンス生成情報を生成（ステップＳ１２５）する。

【００６５】
（ライセンス生成情報送信Ｓ１３０）
ライセンス管理サーバ１００は、ライセンス中継サーバ１１０にライセンス生成情報を送信する。
【００６６】
（処理フォーマットライセンス送信Ｓ１７０）
次に、ライセンス管理サーバ１００は、端末装置１２０に処理フォーマットライセンス５１０を送信する。処理フォーマットライセンス５１０は、送信先の処理フォーマットライセンス判定部に対応したフォーマットであり、本実施の形態では、送信先が、第１のライセンス処理部４２０の処理フォーマットαライセンス判定部４４０の場合について記述するため、処理フォーマットαの処理フォーマットライセンス５１０である。
【００６７】
尚、処理フォーマットαと異なる処理フォーマットライセンス５１０を送信する場合でも、送信先が処理フォーマットαライセンス判定部４４０と異なるが、同様な効果が得られる。
尚、処理フォーマットライセンス５１０の送信は、端末装置１２０からの要求に応じてライセンス管理サーバ１００が送信する場合と、ライセンス管理サーバ１００がブロードキャストした処理フォーマットライセンス５１０を端末装置１２０が受信する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で処理フォーマットライセンス５１０を送受信しても同様な効果が得られる。
【００６８】
尚、端末装置１２０に複数の処理フォーマットライセンス判定部がある場合でも、それぞれのＤＲＭ方式および処理フォーマットで規定された送受信プロトコルにより処理フォーマットライセンス判定部を特定する場合と、処理フォーマットライセンス５１０に記述した識別子、例えば、本実施の形態の＜ｄｒｍＩＤ＞および＜ｖｅｒｓｉｏｎ＞などにより処理フォーマットライセンス判定部を特定する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で処理フォーマットライセンス判定部を特定しても同様な効果が得られる。
【００６９】
図１２を用いてライセンス中継サーバ１１０の処理について説明する。
（ライセンス生成情報受信Ｓ１４０）
ライセンス中継サーバ１１０は、ライセンス管理サーバ１００から、ライセンス生成情報を受信する。
【００７０】
（伝送フォーマットライセンス生成Ｓ１５０）
ライセンス中継サーバ１１０は、ライセンス生成情報から変換フォーマット指定情報７１１に対応するフォーマットでライセンス本体７５０を生成し、変換フォーマット指定情報７１１と、処理フォーマット署名７１２と、改ざん検出７６０を付加して、伝送フォーマットライセンス７１０を生成（Ｓ１５１）する。
【００７１】
尚、本実施の形態では、伝送路Ｎにおける改ざんを検出するために、伝送フォーマットライセンス７１０にライセンス中継サーバ１１０が付加した改ざん検出７６０を含むが、伝送路Ｎにおける改ざん検出を行わないなど、伝送フォーマットライセンス７１０の送受信方法によっては伝送フォーマットライセンス７１０に改ざん検出７６０がなくても同様な効果が得られる。
【００７２】
ライセンス管理サーバ１００が複数の処理フォーマットに対応しており、ライセンス中継サーバ１１０が複数の伝送フォーマットに対応している場合は、ライセンス中継サーバ１１０は、各処理フォーマットおよび各伝送フォーマットに対して、内容が同一の伝送フォーマットライセンス７１０の生成を繰り返す（ステップＳ１５２）。

（伝送フォーマットライセンス送信Ｓ１８０）
次に、ライセンス中継サーバ１１０は、端末装置１２０に伝送フォーマットライセンス７１０を送信する。伝送フォーマットライセンス７１０は、送信先の伝送フォーマットライセンス変換部に対応したフォーマットであり、本実施の形態では、送信先が、第１のライセンス処理部４２０の伝送フォーマットＡライセンス変換部４３０の場合について記述するため、伝送フォーマットＡライセンスの伝送フォーマットライセンス７１０となる。

【００７３】
尚、伝送フォーマットＡと異なる伝送フォーマットライセンス７１０を送信する場合でも、送信先が伝送フォーマットＡライセンス変換部４３０と異なるが、同様な効果が得られる。
尚、伝送フォーマットライセンス７１０の送信は、端末装置１２０からの要求に応じてライセンス中継サーバ１１０が送信する場合と、ライセンス中継サーバ１１０がブロードキャストした伝送フォーマットライセンス７１０を端末装置１２０が受信する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で伝送フォーマットライセンス７１０を送受信しても同様な効果が得られる。

【００７４】
尚、端末装置１２０に複数の伝送フォーマットライセンス変換部がある場合でも、それぞれのＤＲＭ方式および伝送フォーマットで規定された送受信プロトコルにより伝送フォーマットライセンス変換部を特定する場合と、伝送フォーマットライセンス７１０に記述した識別子、例えば、本実施の形態のｄｒｍＩＤ７１６およびｖｅｒｓｉｏｎ７１９など、により伝送フォーマットライセンス変換部を特定する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で伝送フォーマットライセンス変換部を特定しても同様な効果が得られる。

【００７５】
図１３を用いて端末装置１２０の処理について説明する。
（コンテンツ受信Ｓ１９０）
端末装置１２０は、コンテンツ配信サーバ１３０から暗号化コンテンツ８１０を受信する。
（処理フォーマットライセンス受信Ｓ２００）
端末装置１２０の第１のライセンス処理部４２０の処理フォーマットαライセンス判定部４４０は、処理フォーマットαで記述された処理フォーマットライセンス５１０をライセンス管理サーバ１００から受信する。

【００７６】
（ライセンス判定Ｓ２１０）
処理フォーマットαライセンス判定部４４０は、受信した処理フォーマットライセンス５１０を、処理フォーマット署名５１２で検証（ステップＳ２１１）する。
尚、本発明は、特定の署名検証方法に依存しないため、少なくとも、署名検証に用いる公開鍵証明書およびＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）が取得できれば、どのような署名検証方法を用いても同様な効果が得られる。

【００７７】
改ざんが検出されるなど、署名検証に失敗した場合には、コンテンツ利用を中止（ステップＳ４００）する。
改ざんされていないことが確認されると、処理フォーマットαライセンス判定部４４０は、処理フォーマットライセンス５１０から２００３年８月３１日１２時３４分５６秒まで、最大９回利用可能であることを把握し、例えば、現在時刻が２００３年８月１日１２時３４分５６秒で、初回利用であるため、利用可能であると判定（ステップＳ２１２）し、コンテンツ処理部４５０にコンテンツ鍵とコンテンツ処理部でのコンテンツ利用を規定する利用条件を送信する。

【００７８】
利用不可と判定した場合は、コンテンツ利用を中止（ステップＳ４００）する。

尚、本発明は、時刻および利用回数などに関して、特定の判定方法に依存しないため、少なくとも不正な判定が防止できれば、どのような判定方法を用いても同様な効果が得られる。

【００７９】

（コンテンツ利用Ｓ２２０）

コンテンツ処理部４５０は、コンテンツ鍵で暗号化コンテンツ８１０を復号し、利用条件に基づいてコンテンツ利用を制御する。

【００８０】

尚、利用条件にコンテンツＩＤを格納すれば、コンテンツ利用前にライセンスとコンテンツとの対応関係の検証も可能となる。

（伝送フォーマットライセンス受信Ｓ２３０）

端末装置１２０の第１のライセンス処理部４２０の伝送フォーマットＡライセンス変換部４３０は、伝送フォーマットＡで記述された伝送フォーマットライセンス７１０をライセンス中継サーバ１１０から受信する。

【００８１】

（変換処理Ｓ２４０）

伝送フォーマットＡライセンス変換部４３０は、受信した伝送フォーマットライセンス７１０を改ざん検出７６０で改ざん検出（ステップＳ２４１）し、改ざんが検出された場合には、コンテンツ利用を中止（ステップＳ４００）する。

改ざんされていない場合には、伝送フォーマットＡライセンス変換部４３０は、伝送フォーマットライセンス７１０の変換フォーマット指定情報７１１に基づき、伝送フォーマットライセンス７１０を、処理フォーマットライセンス５１０に変換（ステップＳ２４２）する。本実施の形態では、変換フォーマット指定情報７１１に処理フォーマットαを特定する識別子が含まれており、伝送フォーマットＡの伝送フォーマットライセンス７１０は、処理フォーマットαの処理フォーマットライセンス５１０に変換される。

【００８２】

尚、本発明は、特定のフォーマット変換方法に依存せず、少なくとも、伝送フォーマットライセンス７１０をフォーマット変換後、ライセンス管理サーバ１００で生成した処理フォーマットライセンス５１０と一致すれば、どのようなフォーマット変換方法を用いても同様な効果が得られる。

尚、本実施の形態では、変換フォーマット指定情報７１１で伝送フォーマットＡライセンス変換部４３０が変換する処理フォーマットを指定しているが、伝送フォーマットＡライセンス変換部４３０に変換テーブルがあらかじめ設定されている場合では、伝送フォーマットライセンス７１０に変換フォーマット指定情報７１１がなくても伝送フォーマットライセンス７１０から処理フォーマットライセンス５１０にフォーマット変換可能であり同様な効果が得られる。

【００８３】

尚、伝送フォーマットライセンス変換部および処理フォーマットライセンス判定部は、ライセンスフォーマットの変更などに対応する場合には、ライセンス管理サーバ１００およびライセンス中継サーバ１１０などからのダウンロード、または、物理的なモジュールの置き換えによりアップデートする。

フォーマット変換後は、ライセンス管理サーバ１００が生成したライセンスＩＤでライセンスを管理できるため、伝送フォーマットＡライセンスのｌｉｃｅｎｓｅＩＤ７２２が処理フォーマットライセンス５１０のライセンスＩＤと異なる場合でも、ライセンス管理サーバ１００が端末装置１２０のライセンスを統一的に管理できる。

【００８４】

（ライセンス判定Ｓ２５０）

処理フォーマットαライセンス判定部４４０は、受信した処理フォーマットライセンス５１０を、処理フォーマット署名５１２で検証（ステップＳ２５１）する。

尚、本発明は、特定の署名検証方法に依存しないため、少なくとも、署名検証に用いる

公開鍵証明書およびＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）が取得できれば、どのような署名検証方法を用いても同様な効果が得られる。

【００８５】

改ざんが検出されるなど、署名検証に失敗した場合には、コンテンツ利用を中止する。

改ざんされていないことが確認されると処理フォーマットαライセンス判定部４４０は、処理フォーマットライセンス５１０から２００３年８月３１日１２時３４分５６秒まで、最大９回利用可能であることを把握し、例えば、現在時刻が２００３年８月１日１２時３４分５６秒で、初回利用であるため、利用可能であると判定（ステップＳ２５２）し、コンテンツ処理部４５０にコンテンツ鍵とコンテンツ処理部でのコンテンツ利用を規定する利用条件を送信する。

利用不可と判定した場合は、コンテンツ利用を中止（ステップＳ４００）する。

（コンテンツ利用Ｓ２６０）

コンテンツ処理部４５０は、コンテンツ鍵で暗号化コンテンツ８１０を復号し、利用条件に基づいてコンテンツ利用を制御する。

【産業上の利用可能性】

【００８６】

本発明にかかるコンテンツ配信システム１は、変換フォーマット指定情報７１１を有し、端末装置１２０での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスも、端末装置１２０のフォーマット変換手段が、ライセンスに含まれる変換フォーマット指定情報７１１により指定されるフォーマットのライセンスに変換するため、ライセンス発行者による端末装置１２０におけるライセンスの処理フォーマットの指定と、端末装置における受信後のライセンス処理の共通化が可能なコンテンツ配信システムとして有用である。

【００８７】

また、本発明にかかるコンテンツ配信システム１は、処理フォーマット署名７１２を有し、端末装置１２０での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスを処理に用いるフォーマットに変換した後にデジタル署名によるライセンスの改ざん検出が可能なコンテンツ配信システムとして有用である。

さらに、本発明にかかるコンテンツ配信システム１は、フォーマット変換後もライセンス管理サーバ１００が生成したライセンスＩＤと同じライセンスＩＤを用いることにより、異なるフォーマットで配信されたライセンスでもライセンス管理サーバ１００が端末装置１２０のライセンスを統一的に管理することが可能なコンテンツ配信システムとして有用である。

【図面の簡単な説明】

【００８８】

【図１】本発明の実施の形態に係るコンテンツ配信システム１の全体の概略構成を示す図である。

【図２】本発明の実施の形態におけるライセンス管理サーバ１００の構成を示す図である。

【図３】本発明の実施の形態におけるライセンス中継サーバ１１０の構成を示す図である。

【図４】本発明の実施の形態における端末装置１２０の耐タンパ部４１０の構成を示す図である。

【図５】処理フォーマットライセンス５１０の記述例である。

【図６】ＸＭＬ言語によるライセンス本体５１１と処理フォーマット署名５１２の記述例である。

【図７】伝送フォーマットライセンス７１０の記述例である。

【図８】暗号化コンテンツ８１０の構造図である。

【図９】コンテンツ配信システム１におけるライセンスの作成までの処理概略を示すフロー図である。

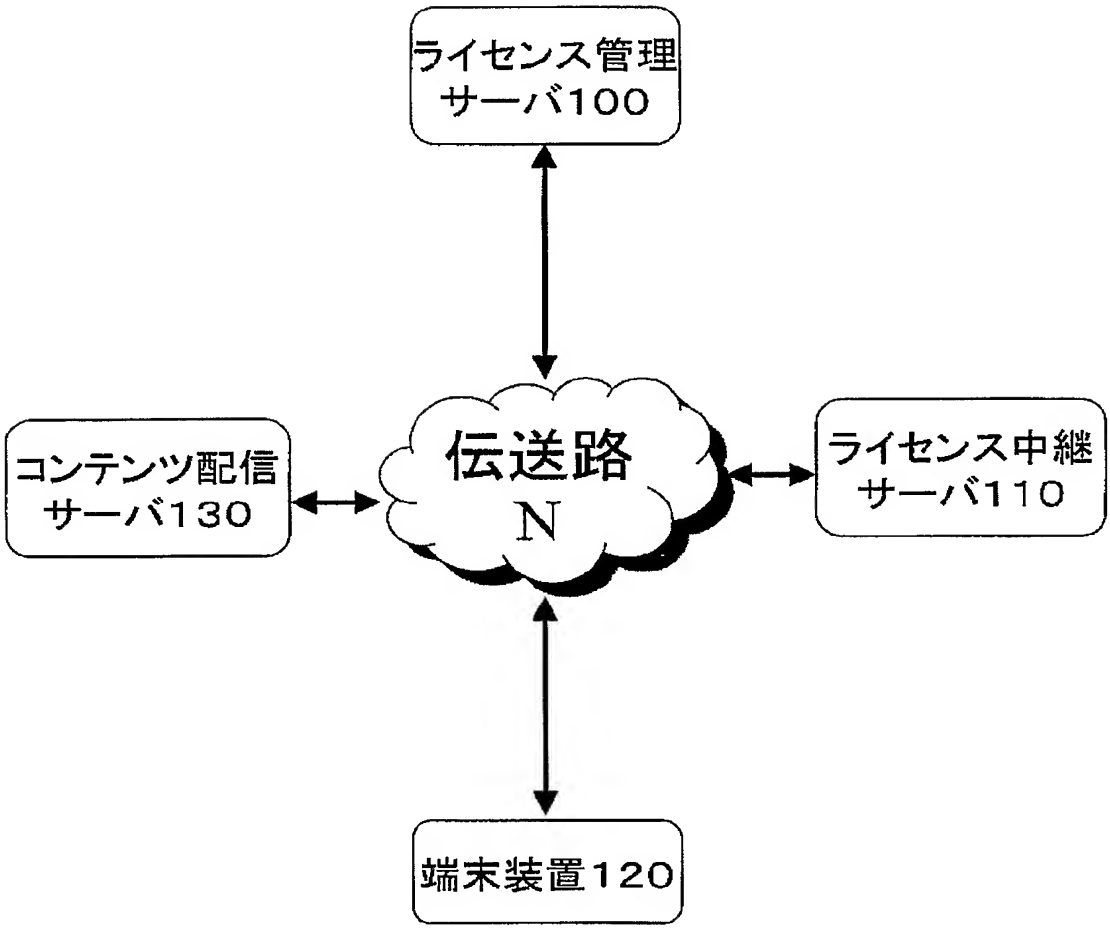
【図１０】コンテンツ配信システム１における暗号化コンテンツとライセンスの配信からコンテンツ利用までの処理概略を示すフロー図である。
【図１１】ライセンス管理サーバ１００の処理を示すフロー図である。
【図１２】ライセンス中継サーバ１１０の処理を示すフロー図である。
【図１３】端末装置１２０の処理を示すフロー図である。

【符号の説明】

【００８９】

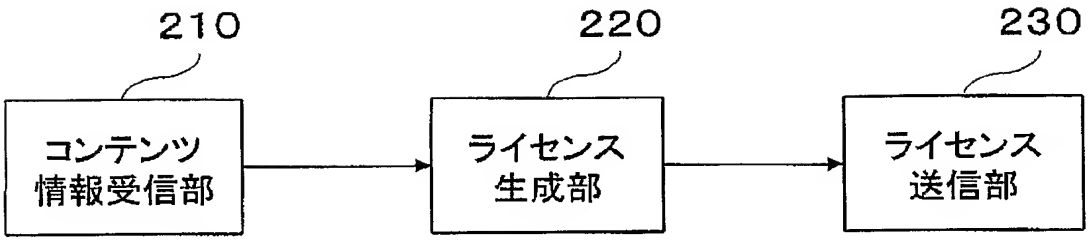
１　コンテンツ配信システム
１００　ライセンス管理サーバ
１１０　ライセンス中継サーバ
１２０　端末装置
１３０　コンテンツ配信サーバ
２１０　コンテンツ情報受信部
２２０　ライセンス生成部
２３０　ライセンス送信部
３１０　ライセンス生成情報受信部
３２０　ライセンス変換部
３３０　ライセンス送信部
４１０　耐タンパ部
４２０　第１のライセンス処理部
４２１　第２のライセンス処理部
４３０　伝送フォーマットＡライセンス変換部
４３１　伝送フォーマットＢライセンス変換部
４４０　処理フォーマットαライセンス処理部
４４１　処理フォーマットβライセンス処理部
４５０　コンテンツ処理部

【書類名】図面
【図１】

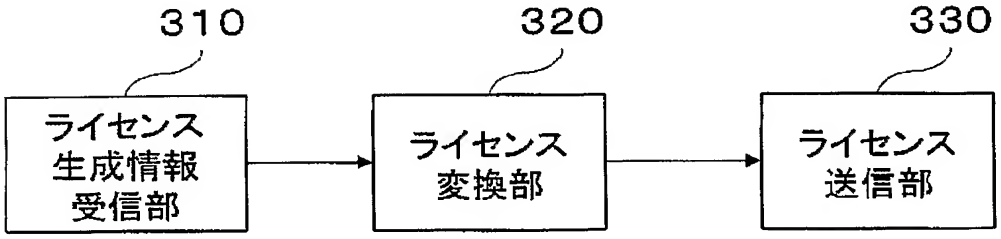


コンテンツ配信システム1

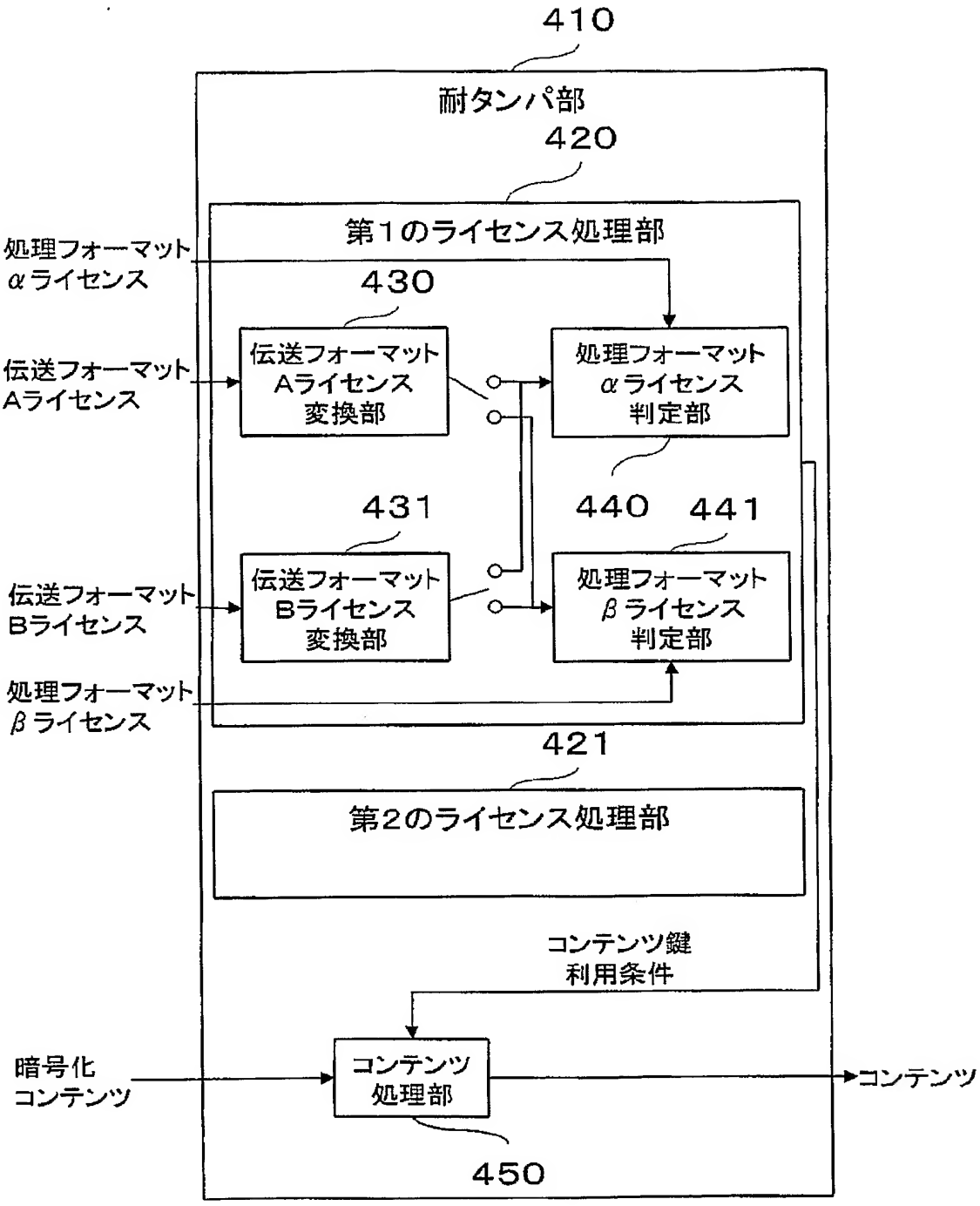
【図２】


210
220
230
コンテンツ
情報受信部
ライセンス
生成部
ライセンス
送信部

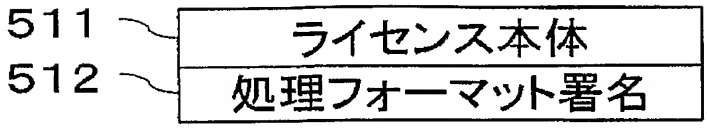
【図３】


310
320
330
ライセンス
生成情報
受信部
ライセンス
変換部
ライセンス
送信部

【図４】


410
耐タンパ部
420
第1のライセンス処理部
処理フォーマット
αライセンス
430
伝送フォーマット
Aライセンス
伝送フォーマット
Aライセンス
変換部
処理フォーマット
αライセンス
判定部
431
440
441
伝送フォーマット
Bライセンス
伝送フォーマット
Bライセンス
変換部
処理フォーマット
βライセンス
判定部
処理フォーマット
βライセンス
421
第2のライセンス処理部
コンテンツ鍵
利用条件
暗号化
コンテンツ
コンテンツ
処理部
コンテンツ
450

【図５】



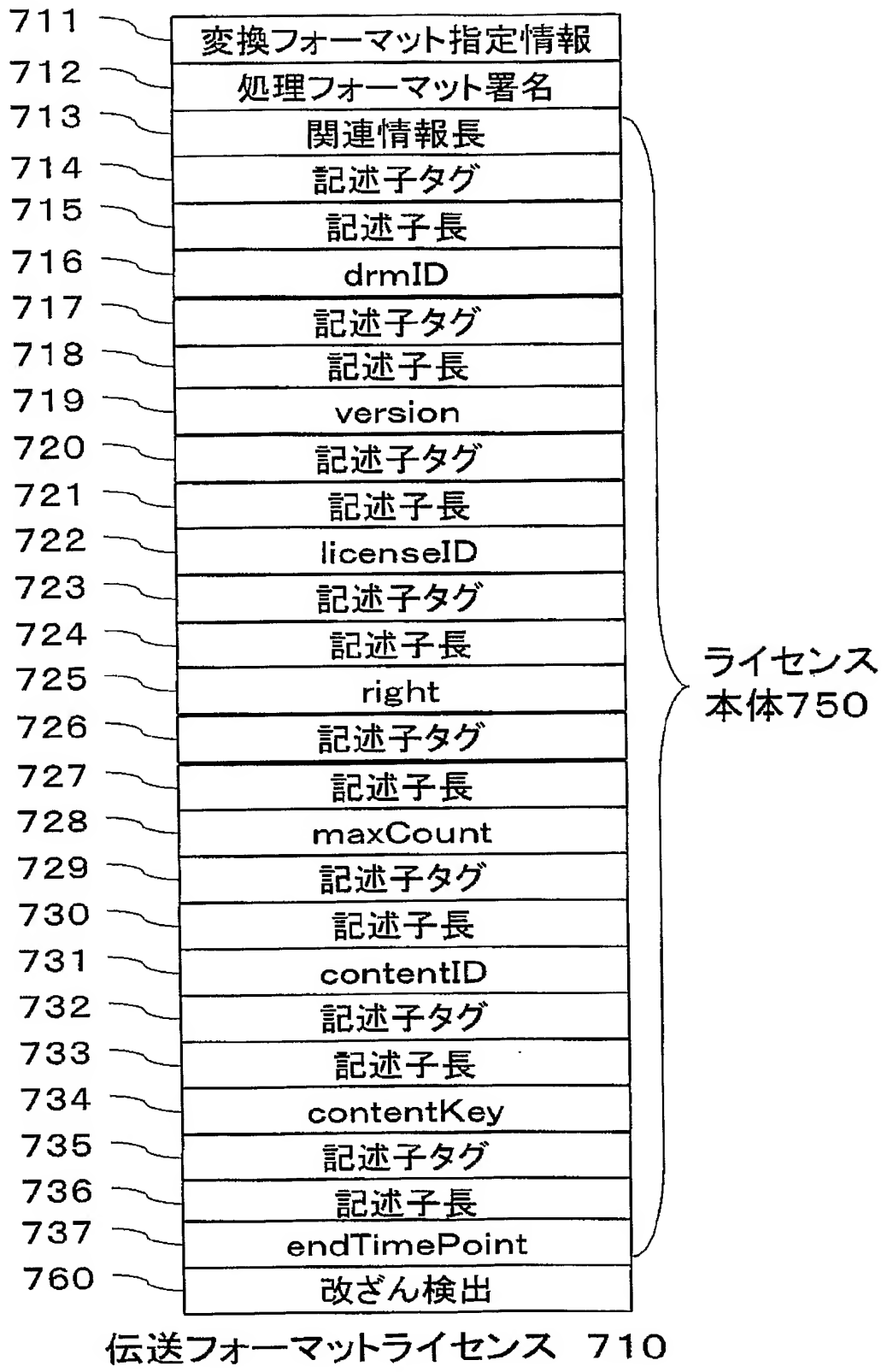
処理フォーマットライセンス　510

【図６】

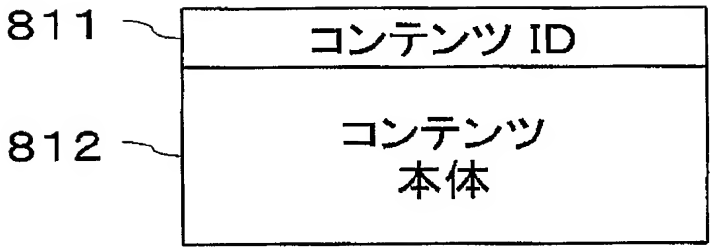
```
<license>
  <grantGroup>
    <grantGroup>
      <GrantGroup>
        <grant>
          <Grant>
            <right><play_main/></right>
            <resource>
              <resourceContent>
                <contentID>02</contentID>
                <contentKey>0001</contentKey>
              </resourceContent>
            </resource>
            <allConditions>
              <condition>
                <exerciseLimit>
                  <maxCount>9</maxCount>
                </exerciseLimit>
              </condition>
            </allConditions>
          </Grant>
        </grant>
      </GrantGroup>
    </grantGroup>
  </grantGroup>
  <licenseGeneralInformation>
    <drmID>0001</drmID>
    <version>0100</version>
    <licenseID>02</licenseID>
    <licenseValidityTimePeriod>
      <endTimePoint>20030831123456Z</endTimePoint>
    </licenseValidityTimePeriod>
  </licenseGeneralInformation>
</license>

<signature>0123456789....0123456789</signature>
```

【図７】

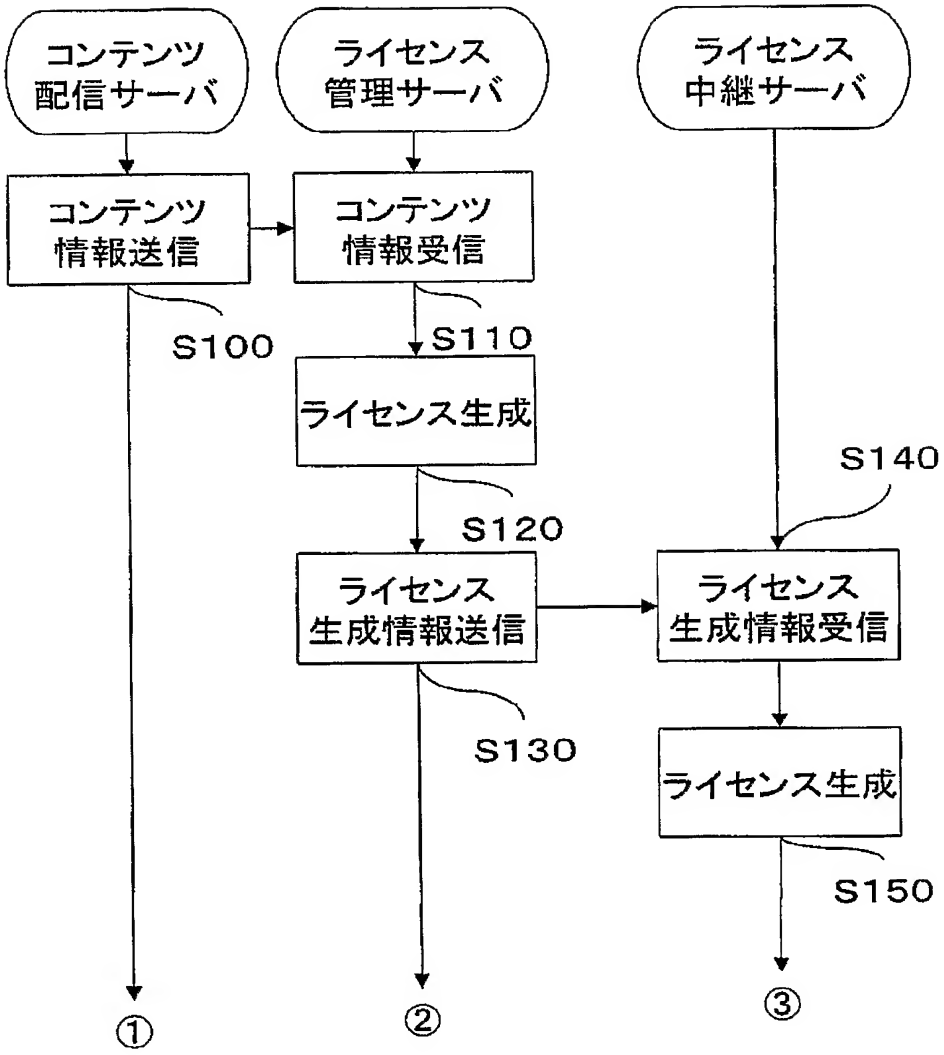

711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
760
変換フォーマット指定情報
処理フォーマット署名
関連情報長
記述子タグ
記述子長
drmID
記述子タグ
記述子長
version
記述子タグ
記述子長
licenseID
記述子タグ
記述子長
right
記述子タグ
記述子長
maxCount
記述子タグ
記述子長
contentID
記述子タグ
記述子長
contentKey
記述子タグ
記述子長
endTimePoint
改ざん検出
ライセンス
本体750
伝送フォーマットライセンス　710

【図８】

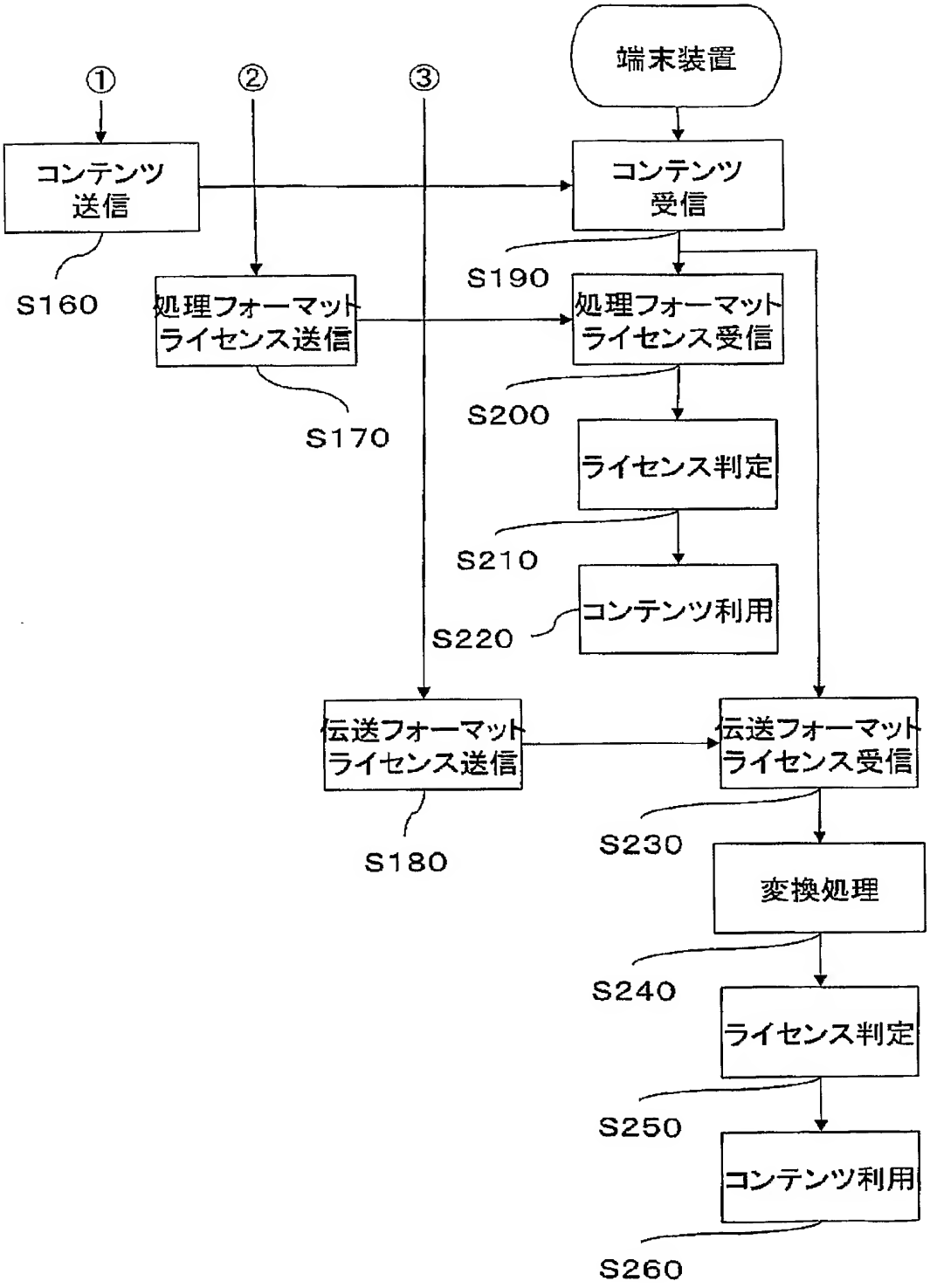


暗号化コンテンツ　810

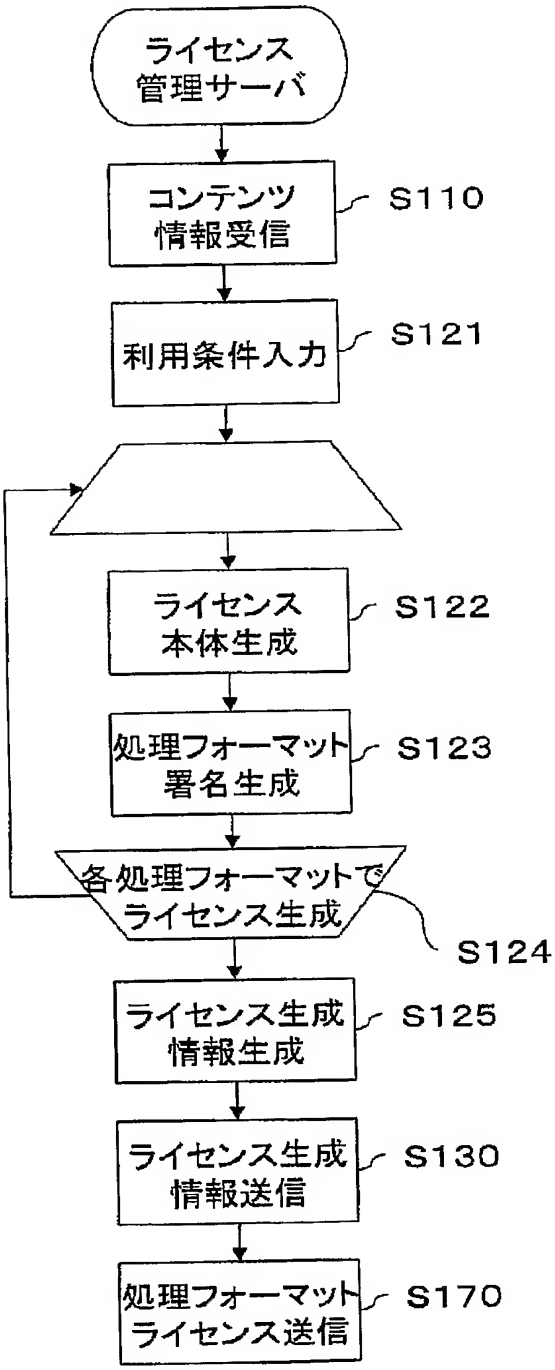
【図９】


コンテンツ
配信サーバ
ライセンス
管理サーバ
ライセンス
中継サーバ
コンテンツ
情報送信
コンテンツ
情報受信
S100
S110
ライセンス生成
S140
S120
ライセンス
生成情報送信
ライセンス
生成情報受信
S130
ライセンス生成
S150
①
②
③

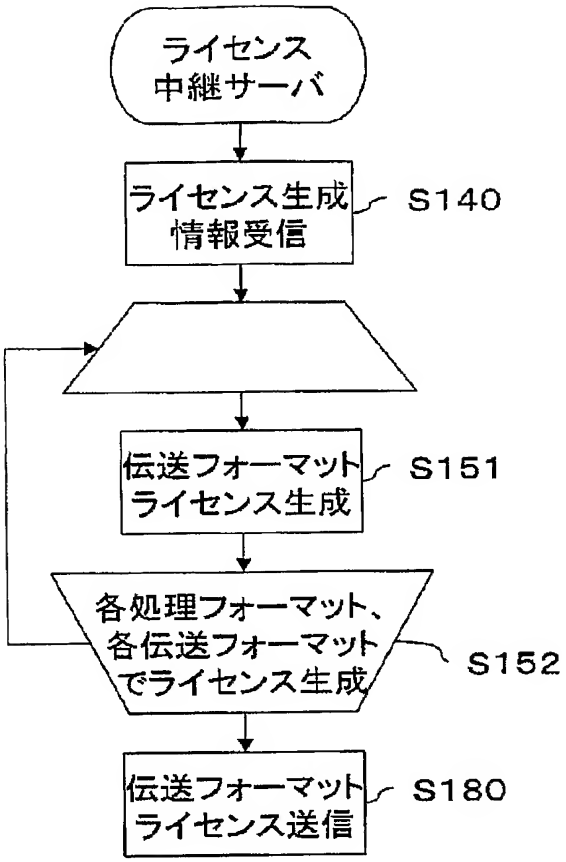
【図１０】


端末装置
①
②
③
コンテンツ送信
コンテンツ受信
S160
S190
処理フォーマットライセンス送信
処理フォーマットライセンス受信
S170
S200
ライセンス判定
S210
コンテンツ利用
S220
伝送フォーマットライセンス送信
伝送フォーマットライセンス受信
S180
S230
変換処理
S240
ライセンス判定
S250
コンテンツ利用
S260

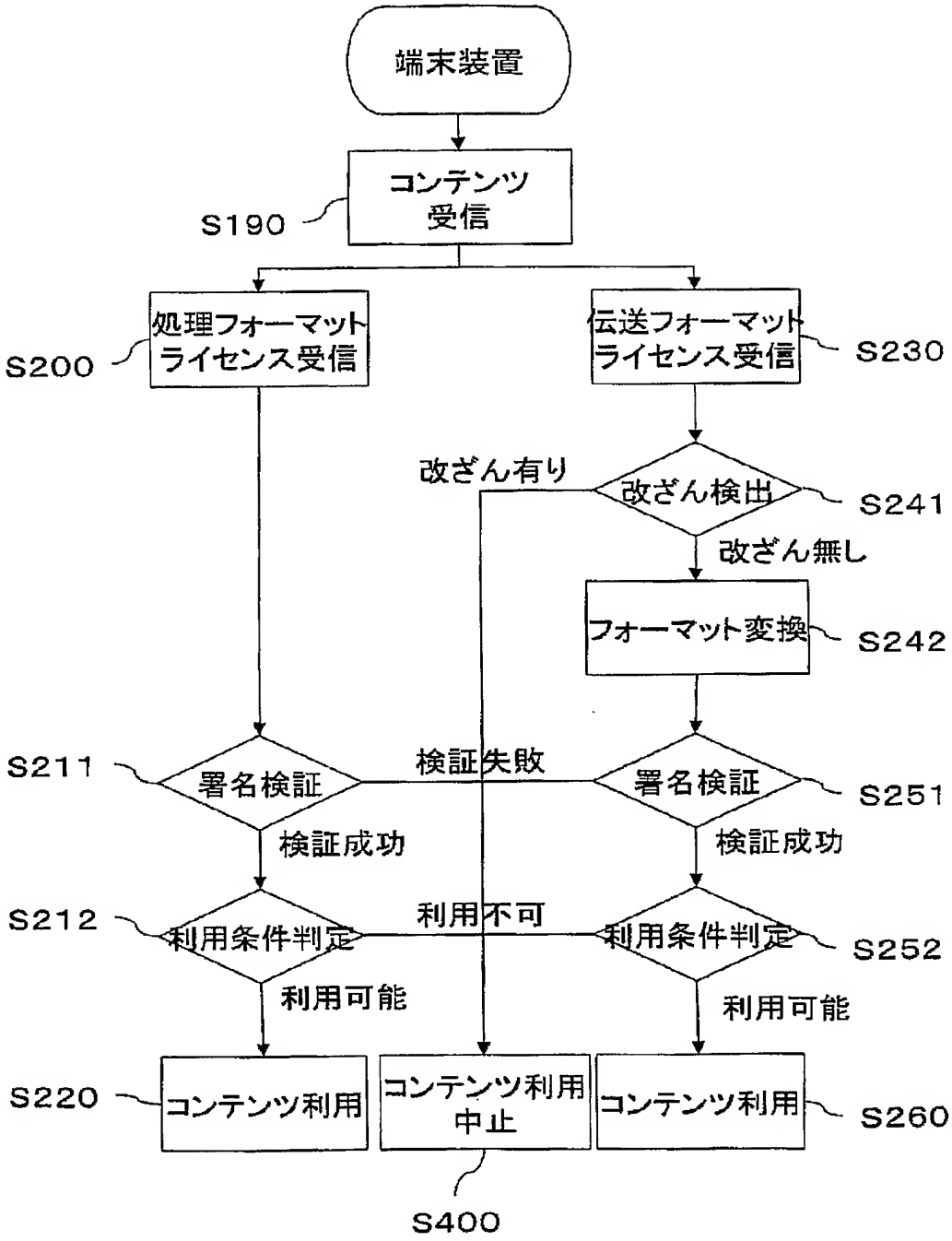
【図１１】


ライセンス
管理サーバ
コンテンツ
情報受信
S110
利用条件入力
S121
ライセンス
本体生成
S122
処理フォーマット
署名生成
S123
各処理フォーマットで
ライセンス生成
S124
ライセンス生成
情報生成
S125
ライセンス生成
情報送信
S130
処理フォーマット
ライセンス送信
S170

【図１２】


ライセンス
中継サーバ
ライセンス生成
情報受信
S140
伝送フォーマット
ライセンス生成
S151
各処理フォーマット、
各伝送フォーマット
でライセンス生成
S152
伝送フォーマット
ライセンス送信
S180

【図１３】


端末装置
コンテンツ受信
S190
処理フォーマットライセンス受信
S200
伝送フォーマットライセンス受信
S230
改ざん有り
改ざん検出
S241
改ざん無し
フォーマット変換
S242
S211
署名検証
検証失敗
署名検証
S251
検証成功
検証成功
S212
利用条件判定
利用不可
利用条件判定
S252
利用可能
利用可能
S220
コンテンツ利用
コンテンツ利用中止
コンテンツ利用
S260
S400

【書類名】要約書
【要約】
【課題】　端末装置で受信したライセンスのフォーマットを変換する場合でも、ライセンス発行者の指定したフォーマットに変換し、フォーマット変換後のライセンスの改ざん検出が可能なコンテンツ配信システムを提供する。
【解決手段】　伝送フォーマットＡライセンス変換部４３０が、ライセンス変換部伝送フォーマットライセンス７１０を変換フォーマット指定情報７１１で指定される処理フォーマットライセンス５１０に変換し、処理フォーマット署名７１２で署名検証することで改ざん検出する。
【選択図】　図４

認定・付加情報

特許出願の番号	特願２００４－００３４３１
受付番号	５０４０００２７９９２
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　１月　９日

＜認定情報・付加情報＞

【提出日】　平成16年 1月 8日

特願２００４－００３４３１

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社